3-6-00

A

Please type a plus sign (+) inside this box [+]

PTO/SB/05 (12/97)
Approved for use through 09/30/00. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b)

Attorney Docket No. 004701.P001 Total Pages 3

First Named Inventor or Application Identifier Chee-Seng Chow

Express Mail Label No. EL 234 215 995 US

ADDRESS TO: **Assistant Commissioner for Patents**
Box Patent Application
Washington, D. C. 20231

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents.

1. X Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. X Specification (Total Pages 26)
(preferred arrangement set forth below)
- Descriptive Title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claims
- Abstract of the Disclosure

3. X Drawings(s) (35 USC 113) (Total Sheets 9)

4. ____ Oath or Declaration (Total Pages 5) (Executed)

a. ___ Newly Executed (Original or Copy)

b. ___ Copy from a Prior Application (37 CFR 1.63(d))
(for Continuation/Divisional with Box 17 completed) **(Note Box 5 below)**

i. ___ DELETIONS OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

5. ____ Incorporation By Reference (useable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. ____ Microfiche Computer Program (Appendix)

7. _____ Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. ____ Computer Readable Copy
b. ____ Paper Copy (identical to computer copy)
c. ____ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. _____ Assignment Papers (cover sheet & documents(s))

9. _____ a. 37 CFR 3.73(b) Statement (where there is an assignee)

__X__ b. Power of Attorney (Unexecuted)

10. _____ English Translation Document (if applicable)

11. _____ a. Information Disclosure Statement (IDS)/PTO-1449

_____ b. Copies of IDS Citations

12. _____ Preliminary Amendment

13. __X__ Return Receipt Postcard (MPEP 503) (Should be specifically itemized)

14. _____ a. Small Entity Statement(s)

_____ b. Statement filed in prior application, Status still proper and desired

15. _____ Certified Copy of Priority Document(s) (if foreign priority is claimed)

16. X___ Other: Attorney signature page including Copy of postcard and Certificate of Express Mailing pursuant to CFR §1.10.

17. **If a CONTINUING APPLICATION,** check appropriate box and supply the requisite information:

___ Continuation ____ Divisional ____ Continuation-in-part (CIP)

of prior application No:_____

18. **Correspondence Address**

_____ Customer Number or Bar Code Label _____
(Insert Customer No. or Attach Bar Code Label here)

or

__X__ Correspondence Address Below

NAME Dennis A. Nicholls, Reg. No. 42,036

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

ADDRESS 12400 Wilshire Boulevard

Seventh Floor

CITY Los Angeles STATE California ZIP CODE 90025-1026

Country U.S.A. TELEPHONE (408) 720-8598 FAX (408) 720-9397

PTO/SB/05 (12/97)
Approved for use through 09/30/00. *OMB 0651-0032*
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: 3 March, 2000 By Dennis A. Nicholls
Dennis A. Nicholls
Reg. No. 42,036

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026
(408) 720-8598

"Express Mail" mailing label number: EL 234 215 995 US
Date of Deposit: March 3, 2000
I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231

Tina Domingo
(Typed or printed name of person mailing paper or fee)

(Signature of person mailing paper or fee)

3-3-2000
(Date signed)

Serial/Patent No.: * * Filing/Issue Date: Herewith
Client: GetThere.com
Title: System and Method For Accessing A Remote Server From An Intranet With A Single Sign-On
BSTZ File No.: 004701.P001 Atty/Secty Initials: JHS/DAN/td
Date Mailed: 3-3-2000 Docket Due Date: * *

The following has been received in the U.S. Patent & Trademark Office on the date stamped hereon:

- ☐ Amendment/Response (____ pgs.)
- ☐ Appeal Brief (____ pgs) (in triplicate)
- XX Application - Utility (26 pgs , with cover and abstract)
- ☐ Application - Rule 1 53(b) Continuation (____ pgs.)
- ☐ Application - Rule 1 53(b) Divisional (____ pgs)
- ☐ Application - Rule 1 53(b) CIP (____ pgs)
- ☐ Application - Rule 1 53(d) CPA Transmittal (____ pgs.)
- ☐ Application - Design (____ pgs)
- ☐ Application - PCT (____ pgs.)
- ☐ Application - Provisional (____ pgs.)
- ☐ Assignment and Cover Sheet
- XX Certificate of Mailing (Express Mail)
- XX Declaration & POA (5 pgs.) (Unexecuted)
- ☐ Disclosure Docs & Org & Copy of Inventor's Signed Letter(____pgs)
- XX Drawings 9 # of sheets includes 10 figures
- ☒ Express Mail No. EL234215995US
- ☐ ____ Month(s) Extension of Time
- ☐ Information Disclosure Statement & PTO-449 (__ pgs.)
- ☐ Issue Fee Transmittal
- ☐ Notice of Appeal
- ☐ Petition for Extension of Time
- ☐ Petition for ____
- ☒ Postcard
- ☐ Power of Attorney (____ pgs.)
- ☐ Preliminary Amendment (____ pgs.)
- ☐ Reply Brief (____ pgs.)
- ☐ Response to Notice of Missing Parts
- ☐ Small Entity Declaration for Indep. Inventor/Small Business
- ☒ Transmittal Letter, in duplicate (3 pages)
- ☒ Fee Transmittal, in duplicate

☒ Check No. 34047
Amt. $804.00

☐ Check No. ____
Amt. ____

☐ Other: ____

Patent

UNITED STATES PATENT APPLICATION

FOR

SYSTEM AND METHOD FOR ACCESSING A REMOTE SERVER FROM AN INTRANET WITH A SINGLE SIGN-ON

INVENTORS:

CHEE-SENG CHOW
JAMES SUNG
JEROME TSUNG-YAO CHEN
FIYAZ SUNDARJI

PREPARED BY:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1026

(408) 720-8300

ATTORNEY'S DOCKET NO. 004701.P001

Express Mail Certificate

"Express Mail" mailing label number: EL 234 215 995 US
Date of Deposit: March 3, 2000
I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Assistant Commissioner for Patents, Washington, D. C. 20231

Tina Domingo
(Typed or printed name of person mailing paper or fee)

(Signature of person mailing paper or fee)

3-3-2000
(Date signed)

SYSTEM AND METHOD FOR ACCESSING A REMOTE SERVER FROM AN INTRANET WITH A SINGLE SIGN-ON

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to and claims the benefit of the filing date of U.S. Provisional Patent Application number 60/122,912, filing date 03/05/1999, entitled "Unified Single Sign On".

FIELD OF THE INVENTION

The present invention relates to wide area networking, and, more specifically, to accessing a remote server from an Intranet utilizing a single sign-on authentication.

BACKGROUND

In order to be able to access various computer resources, such as the Internet, a private network such as an Intranet, or other similar resources, a user must authenticate his right to access the resource through a process variously called a "log-on" or a "sign-on". A typical process includes submitting an agreed upon name called a "username" and a password. Usually the submission is performed by the user typing in his username and password on an electronic form supplied by the resource.

Many companies have created private networks that mimic the activity of the Internet. These private networks, called Intranets, allow authorized users access to data which the company wishes to keep

private. A software structure called a firewall allows a one-way access from an Intranet to the Internet. The firewall allows authorized users of that Intranet to access data from the Internet without allowing external persons on the Internet to access the private Intranet data.

In order to access these Intranets, authorized users sign-on with a username and a password. However, these same users may then wish to access remote servers on the Internet. These remote servers may require their own sign-on authentication for the user.

Each particular user may have a different username for the sign-on for the remote server than for the Intranet. Furthermore, for the sake of maximum security, a different password should be used. However, what has been noticed in practice is that the requirement for multiple usernames and passwords often produces non-secure behavior in many users. They may either use the same password in both situations, or them may use trivial passwords (e.g. "password"). Other forms of non-secure behavior may include writing down the usernames and passwords, and posting these on a user's computer workstation.

SUMMARY OF THE INVENTION

A system and method for performing multiple user authentications with a single sign-on is disclosed. In one exemplary embodiment, the system and method starts when the user performs a first user authentication, with user name and password, within the user's Intranet. Then the user selects a remote server subsequent to the first authentication. The server in the Intranet sends a token to the remote server containing authentication information made available because of the first authentication. Finally, the remote server decodes the authentication information, which has the effect within the remote server of performing a second user authentication without the user needing to sign-on a second time.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings:

FIG. 1 is a block diagram of a method for accessing a remote server with a single sign-on authentication, according to one embodiment of the present invention.

FIG. 2A is an exemplary screen of a user sign-on interface, according to one embodiment of the present invention.

FIG. 2B is an exemplary screen of a user access link to a remote server, according to one embodiment of the present invention.

FIG. 3 is a diagram illustrating software module location within hardware configuration items, according to one embodiment of the present invention.

FIG. 4 is a block diagram of the Intranet server, according to one embodiment of the present invention.

FIG. 5 is a block diagram of the remote server, according to one embodiment of the present invention.

FIG. 6 is table showing contents of an authentication token, according to one embodiment of the present invention.

FIG. 7 is a flowchart of the authentication method, according to one embodiment of the present invention.

FIG. 8 is a flowchart of a method for adding a new user, according to one embodiment of the present invention.

FIG. 9 is a flowchart of a method for updating a user's profile, according to one embodiment of the present invention.

DETAILED DESCRIPTION

A system and method for performing multiple user authentications with a single sign-on is disclosed. In one embodiment, the system and method starts when the user performs a first user authentication, with user name and password, within the user's Intranet. Then the user selects a remote server subsequent to the first authentication. The server in the Intranet sends a token to the remote server containing authentication information made available because of the first authentication. Finally, the remote server decodes the authentication information, which has the effect within the remote server of performing a second user authentication without the user needing to sign-on a second time.

Referring now to Figure 1, a block diagram of a method for accessing a remote server with a single sign-on authentication is shown, according to one embodiment of the present invention. Figure 1 illustrates an Intranet 102 and a remote server 104. In the Figure 1 embodiment, an Intranet server 120 is shown. This Intranet server 120 may be the server for the internal Intranet of a company. In other embodiments, the functionality of Intranet server 120 may be distributed among several pieces of equipment within Intranet 102.

Intranet 102 may be connected to remote server 104 via the Internet or via another wide area network (WAN). In one exemplary embodiment, remote server 104 may host a travel reservation and booking service. In other embodiments, Intranet 102 may be connected

directly to remote server 104 via a local area network (LAN) or by another kind of computer interface.

It should be noted that remote server 104 is logically remote and not necessarily geographically remote. Remote server 104 may be in the same building as Intranet 102, and may even be connected to Intranet 102 by a direct connection such as a LAN. Being logically remote may merely indicate that remote server 104 may not be immediately accessed by a user connected to Intranet 102 due to sign-on requirements of remote server 104.

In order that a user may become authorized to access an application within remote server 104, the user may first start their browser, at step 110. The Intranet server 120 may then present a sign-on page to the user, at step 112. The user may then click a link on this sign-on page to enter the primary sign-on sequence 116 with Intranet server 120. This primary sign-on sequence 116 may take the form of a forms-driven dialog that prompts the user for the username, password, and, potentially, other forms of identifying data.

In other embodiments, the process of signing-on to the Intranet 102 may be performed by different actions than those shown in steps 110, 112, 114, and 116. In alternate embodiments, the user access to the Intranet may be authorized by other mean, or the user access to the Intranet may be automatically authorized. In one alternate embodiment, a user may sign-on when powering-on their workstation. Once signed on to their workstation, they are automatically authenticated to the Intranet. Each of these alternate embodiments may serve as a primary sign-on sequence of the present invention.

Once a primary sign-on sequence 116 is completed, the user may be presented with the ability to use the resources of the Intranet, and resources external to the Intranet. In one embodiment, a list of links to click on are presented to the user on the user's browser 118. In this embodiment, a link to the remote server is also present.

If the user clicks the link for the remote server 130, then, because the Intranet server 120 has already authenticated the user in the primary sign-on sequence 116, the Intranet server 120 sends information to the remote server 104 which causes the remote server 104 to authenticate the user without the user needing to perform a second sign-on sequence. In one embodiment, the Intranet server 120 sends an encrypted user identification (user ID) and time stamp to the remote server 104. The remote server 104 may decode the user ID and time stamp, and based only upon these items authenticate the user without the need for the user to perform a secondary sign-on sequence 134.

After this authentication is complete, the remote server 104 gives access to the user. In one embodiment, the remote server 104 presents a menu page to the user. This menu page enables the user to access desired functions available through the remote server 104.

It should be noted that the order of certain of the authentication steps shown in Figure 1 is not critical to the present invention. In alternate embodiments, certain steps analogous to the steps 110, 112, 114, 116, 118, and 130 may occur in differing order. In certain embodiments, one or more analogous steps may not be present at all.

Referring now to Figure 2A, an exemplary screen of user sign-on interface is shown, according to one embodiment of the present

invention. The Figure 2A screen may be an Intranet sign-on page 200 for use in the primary sign-on sequence 116 of Figure 1. In other embodiments, other techniques may be used for authenticating a user for access to an Intranet.

Intranet sign-on page 200 may include a user prompt 202 with associated username entry field 204. In one embodiment, the user selects the username entry field 204 and types the username. Intranet sign-on page 200 may also include a password prompt 206 with associated password entry field 208. In one embodiment, the user selects the password entry field 208 and types the password. In alternate embodiments, other kinds of user information may be gathered for the purpose of authentication, including alternate kinds of text, voice entry, or other physical evidence (e.g. fingerprint or retina matching). In each case the Intranet server 120 may provide user authentication subsequent to a action taken by the user.

Referring now to Figure 2B, an exemplary screen of a user access link to a remote server is shown, according to one embodiment of the present invention. The Intranet services page 214 of Figure 2B may be presented to the user to allow the user to access certain features and functions of the Intranet subsequent to a successfully completed sign-on sequence. Intranet services page 214 may include links to Intranet services 216, 218, which, when selected by the user, may cause subsequent features and functions specific to the Intranet to be presented to the user. Links to Intranet services 216, 218 may be to services such as user spending accounts, the company's proprietary

technical database, or any other services provided by the particular Intranet.

Intranet services page 214 may also include a link to remote server 220. In one embodiment, the user selects this link to remote server 220 by clicking on it. This act causes a subsequent page to be displayed to the user to allow the user to access features and functions of the remote server. In alternate embodiments, other dialogs between the user and remote server are used. In each case the user need not provide authentication information as part of a secondary sign-on sequence.

Referring now to Figure 3, a diagram illustrating software module location within hardware configuration items is shown, according to one embodiment of the present invention. Intranet 300 may include a user's browser 308 and Intranet server code 302. In one embodiment, the user's browser 308 and Intranet server code 302 are hosted by separate processors. In this embodiment, user's browser 308 and Intranet server code 302 may exchange information over a user data path 310. In alternate embodiments, user's browser 308 and Intranet server code 302 may be executed upon a shared processor or processors.

In one embodiment, Intranet services code 302 may include a remote server module 304 and an encryption module 306. In one embodiment, remote server module 304 may be a common gateway interface (CGI) module or a server plug-in module. In alternate embodiments, remote server module 304 may utilize other forms of interface code architecture. The remote server module 304 may be activated by a remote link request 312. When activated, remote server module 304 may examine the status of the user's authentication for

access to the Intranet. If the user is authenticated for access to the Intranet, then remote server module 314 may respond to remote link request 312 by providing a uniform resource locator (URL) with encrypted token 314 to the user's browser for use in accessing remote server code 320.

Remote server module 314 may make use of encryption module 306 in the preparation of the URL with encrypted token 314. Encryption module 306 may use the data encryption standard (DES), with keys of various lengths. In one embodiment, encryption module 306 may use the 128 bit long keys for users within the United States, and keys with fewer bits (e.g. 56 bits) for users outside the United States. In one embodiment, triple DES in cipher block chaining (CBC) mode may be used, with two keys. In CBC mode, the token is encrypted with the first key, decrypted with the second key, and then re-encrypted with the first key. Data from one 64 bit long block may be used to seed the initialization vector of the subsequent block.

An example URL with encrypted token 314 may be as follows:

http://www.remoteserver.com/cgi/xreg/remoteserver/corp/abcorp?message_version=1&auth_message={encrypted token}&err_url={Error URL}&fwd_cnt=1 .

Once the user's browser 308 has the URL with encrypted token 314, the user's browser 308 may transmit the URL with encrypted token 314 to the remote server code 320 along a transmitted URL data path 316. Remote server code 320 may include a CGI module 322, a remote

server application 324, and an error handler 326. In one embodiment, CGI module 322 receives the URL with encrypted token from the transmitted URL data path 316. CGI module 322 may then decode the URL and decrypt the encrypted token. In one embodiment, CGI module 322 passes the decrypted token to remote server application 324 for authentication of the user. In other embodiments, the CGI module 322 may perform the authentication of the user.

In alternate embodiments, remote server code 320 may utilize alternate interface code architectures than the CGI shown in the Figure 3 embodiment.

If, based upon the contents of the decrypted token, the remote server application 324 authenticates the user, then a welcoming page 318 is sent to the user's browser. This welcoming page indicates to the user that the user has been authenticated by the remote server code 320. Once the user has been authenticated, the welcoming page may be used by the user to access features and functions of the remote server application 324.

If, based upon the contents of the decrypted token, the remote server application 324 cannot authenticate the user, then the error handler 326 may prepare an error message for transmitting to the user's browser.

Referring now to Figure 4, a block diagram of the Intranet server 400 is shown, according to one embodiment of the present invention. Intranet server 400 may include a server bus 402, a network access circuit 404, a central processing unit (CPU) 406, disk 408, random

access memory (RAM) 410, removable media 412, and read only memory (ROM) 414.

In one embodiment, Intranet server code 302 of Figure 3 may be executed by CPU 406 and may be stored on disk 408. Disk 408 may be magnetic, optical, or magneto-optical. Portions of Intranet server code 302 may be loaded or removed from Intranet server 400 by using removable media 412. Removable media 412 may be a floppy disk, magnetic tape, optical media (e.g. compact disc read only memory (CD-ROM), digital versatile disc (DVD), write once read many (WORM)), flash memory, or any other removable data storage media.

Intranet server 400 may be connected to a wide area network (WAN) 420. In one embodiment, WAN 420 is the Internet. In alternate embodiments, other kinds of WAN may be used. In one embodiment, Intranet server 400 may be connected to WAN 420 via a local area network (LAN) 416 and a gateway 418. Intranet server 400 may use a network access circuit 404 to connect with LAN 416. In other embodiments, Intranet server 400 may connect to WAN 420 via other forms of connections, or may be directly connected to WAN 420.

For the purpose of security within the Intranet, Intranet server 400 may use a security software module called a firewall. The firewall may be contained within Intranet server 400 or may be executed by gateway 418.

Referring now to Figure 5, a block diagram of the remote server 500 is shown, according to one embodiment of the present invention. Remote server 500 may include a server bus 502, a network access circuit 504, a CPU 506, disk 508, RAM 510, removable media 512, and ROM 514.

In one embodiment, remote server code 320 of Figure 3 may be executed by CPU 506 and may be stored on disk 508. Disk 508 may be magnetic, optical, or magneto-optical. Portions of remote server code 320 may be loaded or removed from remote server 500 by using removable media 512. Removable media 512 may be a floppy disk, magnetic tape, optical media (e.g. CD-ROM, DVD, or WORM), flash memory, or any other removable data storage media.

Remote server 500 may be connected to a WAN 520. In one embodiment, WAN 520 is the Internet. In alternate embodiments, other kinds of WAN may be used. In one embodiment, remote server 500 may be connected to WAN 520 via a network access circuit 504. In other embodiments, remote server 500 may connect to WAN 520 via other forms of connections.

Referring now to Figure 6, a table shows the contents of an authentication token, according to one embodiment of the present invention. In the Figure 6 embodiment, the authentication token takes the form of credential token 600. Credential token 600 may include a username 602, an expiration time 604, and checksum 606. Credential token 600 may be encrypted by the Intranet server and placed into a URL for transmission to and subsequent user authentication by the remote server. Username 602 may be any form of agreed-upon name for the user.

Credential token 600 is intended to be encrypted and placed within a URL for transmitting to the remote server. The remote server may authenticate the user based only upon the contents of the URL. A user could circumvent the security access features of the remote server by

bookmarking or otherwise remembering the URL. Such a bookmark would allow unauthorized persons access to the remote server. Therefore, credential token 600 includes an expiration time 604. In one embodiment, expiration time 604 may be the current time within the Intranet server when the credential token 600 is created. Expiration time 604 may be in Unix 32 bit long Unix time code (UTC) format. Synchronization of the time clocks within the Intranet and the remote server may be performed by network time protocol (NTP).

In alternate embodiments, the expiration time 604 contains a representation of some time subsequent to the time of URL generation after which the remote server will no longer accept the URL for the purpose of user authentication. This expiration time 604 may be chosen to be the current time of credential token 600 creation, as indicated by the time clock of the Intranet, plus an additional period of time to allow for the estimated transmission time over the Internet. The expiration time 604 may have added to it an additional time period so that the time standards of the Intranet and of the remote server need not be closely synchronized.

The checksum 606 may be as calculated by one of various cyclic redundancy check (CRC) algorithms, or by any other agreed-upon algorithm. In one embodiment, checksum 606 may be calculated using CRC-32. Checksum 606 may give an indication of data integrity when credential token 600 is examined by the remote server. The results of the remote server examining the credential token 600 may be used to permit or deny user authentication.

Referring now to Figure 7, a flowchart of the authentication method is shown, according to one embodiment of the present invention. The user starts 700 the process by performing an Intranet user authentication 702. When the user selects a link to gain access to the remote server, the Intranet server first forms the necessary token fields, at step 704. These token fields may include the username 602 and expiration time 604 of Figure 6. Then, at step 706, the token fields are concatenated to form a single binary string.

At step 708, a checksum is calculated for the single binary string created in step 706, and the checksum is appended to the binary string. Then, in step 710, the binary string is encrypted. In order that the encrypted binary string may be inserted into a URL, at step 712 the encrypted binary string is converted to American standard code for information interchange (ASCII) format. The result of step 712 is an encrypted token consisting of ASCII characters.

At step 714, the Intranet server places the encrypted ASCII token into a URL. Then, in step 716, the URL containing the encrypted ASCII token is transmitted to the remote server.

The remote server receives the URL and extracts the encrypted ASCII token. In step 718, the remote server reverses the process of steps 710 and 712. In decision step 720, the remote server tests the validity of the received checksum. If the checksum is not valid, then, in step 730, an error message is generated and the user is not authenticated.

If the checksum is valid, then, in decision step 722, the timestamp (expiration time field) is examined. If the indicated time of the timestamp is not within a selected tolerance of the time on the time clock of the

remote server, then, in step 732, an error message is sent, and the user is not authenticated. If the indicated time of the timestamp is within a selected tolerance, then, in step 724, the remote server authenticates the user and issues a welcoming page. In one embodiment, the selected tolerance is between 15 and 25 minutes.

Referring now to Figure 8, a flowchart of a method for adding a new user is shown, according to one embodiment of the present invention. The Figure 7 process assumed that the username corresponded to an existing, valid user of the remote server. The Figure 8 embodiment adds the capability to add new user accounts to the remote server.

In step 802, the user performs an Intranet user authentication. In decision step 804, the Intranet server determines whether the user is a new user. If not, then the process proceeds to step 808. If, however, the user is a new user, in step 806 the Intranet server sets a new user flag.

In alternate embodiments, the Intranet server may not make any determination whether the user is a new user, and may not take any action with regards the new or existing status of the user.

In step 808 the Intranet server forms the fields for the token, including the new user flag. Then, at step 810, the token fields are concatenated to form a single binary string.

At step 812, a checksum is calculated for the single binary string created in step 810, and the checksum is appended to the binary string. Then, in step 814, the binary string is encrypted. In order that the encrypted binary string may be inserted into a URL, at step 816 the

encrypted binary string is converted to ASCII format. The result of step 816 is an encrypted token consisting of ASCII characters.

At step 818, the Intranet server places the encrypted ASCII token into a URL. Then, at step 820, the URL containing the encrypted ASCII token is transmitted to the remote server.

In step 822, the remote server receives and decrypts the token. In decision step 824, the remote server determines whether the checksum is valid and whether the timestamp is within tolerance. If not, then in step 826 an error message is generated and the user is not authenticated.

If, in step 824, the checksum is valid and the timestamp is within tolerance, then, in step 828, the new user flag status is tested. If the new user flag is not set, then the process proceeds to step 840, and the user is authenticated. However, if the new user flag is set, then the process proceeds to decision step 830.

In alternate embodiments, there may be no new user flag, and the remote server software may automatically treat all unknown users as new users. In this alternate embodiment, once the user's authentication credentials are established by a step analogous to step 824 of Figure 8, the remote server software may automatically create a new user account for all unknown users.

If, in step 830, the remote server software is not set to enable adding new users, then, in step 832, an error message is generated and the user is not authenticated. However, if, in step 830, the remote server software is set to enable adding new user, then, in step 834, the remote server tests to see if the username is already in use. If so, then, in step

836, an error message is sent and the user is not authenticated. If, however, in step 834, the username is determined to not be in prior use, then, in step 838, a new user account is established, and, in step 840, the user is authenticated.

Referring now to Figure 9, a flowchart of a method for updating a user's profile is shown, according to one embodiment of the present invention. User profile information may be stored by the remote server. The user profile information may include information about the user that may help the remote server provide efficient service to the user. In one embodiment, the remote server may be a travel reservation and booking service. In this embodiment, user profile information may include dietary choices, seating preferences, travel spending limits, and other information specific to a given user.

The Figure 7 process assumed that the user profile information could only be edited on the remote server. The Figure 9 embodiment adds the capability to transmit new or updated user profile information to the remote server.

In step 902, the user performs an Intranet user authentication. In decision step 904, the Intranet server determines if the user wishes to create a new user profile or update an existing user profile. If not, then the process proceeds to step 908. If, however, the user creates a new user profile or updates an existing user profile, in step 906 the Intranet server places this user profile data into strings.

In step 908, the Intranet server forms the fields for the token, including the new user profile data. Then, at step 910, the token fields are concatenated to form a single binary string.

At step 912, a checksum is calculated for the single binary string created in step 910, and the checksum is appended to the binary string. Then, in step 914, the binary string is encrypted. In order that the encrypted binary string may be inserted into a URL, at step 916 the encrypted binary string is converted to ASCII format. The result of step 916 is an encrypted token consisting of ASCII characters.

At step 918 the Intranet server places the encrypted ASCII token into a URL. Then, at step 920, the URL containing the encrypted ASCII token is transmitted to the remote server.

In step 922, the remote server receives and decrypts the token. In decision step 924, the remote server determines whether the checksum is valid and whether the timestamp is within tolerance. If not, then, in step 926, an error message is generated and the user is not authenticated.

If, in step 924, the checksum is valid and the timestamp is within tolerance, then, in step 928, the token is examined for user profile information. If there is no user profile information present within the token, then the process proceeds to step 940, and the user is authenticated at step 940. However, if user profile information is found, then the process proceeds to decision step 930.

If, in step 930, the remote server software is not set to enable updating user profile information, then, in step 932, an error message is generated and the user is not authenticated. However, if, in step 930, the remote server software is set to enable updating user profile information, then, in step 938, the remote server creates a new user

profile or updates any existing user profile. Then, in step 940, the user is authenticated.

In the foregoing specification, the invention has been described with reference to specific exemplary embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto without departing from the broader spirit and scope of the invention as set forth in the appended claims. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.

CLAIMS

What is claimed is:

1. A method of performing multiple user authentications with a single sign-on, comprising:

performing a first user authentication;

selecting a remote server subsequent to said first authentication;

sending a token to said remote server containing authentication information responsive to said first authentication; and

decoding said authentication information, wherein said decoding said authentication information induces a second user authentication.

2. The method of claim 1, wherein said sending includes sending said token within a universal resource locator.

3. The method of claim 2, wherein said token includes a timestamp.

4. The method of claim 2, wherein said token is encrypted.

5. The method of claim 2, wherein said token includes a new user flag.

6. The method of claim 5, wherein said remote server creates a new user account in response to said new user flag.

7. The method of claim 2, wherein said token includes user profile update information.

8. The method of claim 7, wherein said remote server updates a user profile in response to said user profile update information.

9. The method of claim 1, wherein said first user authentication occurs within an Intranet.

10. The method of claim 1, wherein said second user authentication occurs within said remote server.

11. A system for performing multiple user authentications with a single sign-on, comprising:

a user sign-on interface, configured to perform a first user authentication;

a link interface, configured to select a remote server subsequent to said first user authentication;

a token configured to be sent to said remote server, said token containing authentication information responsive to said first user authentication; and

a decoder configured to decode said authentication information, said decoder further configured to induce a second user authentication.

12. The system of claim 11, wherein said token is coupled to a uniform resource locator.

13. The system of claim 12, wherein said token includes a timestamp.

14. The system of claim 12, wherein said token is encrypted.

15. The system of claim 12, wherein said token includes a new user flag.

16. The system of claim 15, wherein said remote server creates a new user account in response to said new user flag.

17. The system of claim 12, wherein said token includes user profile update information.

18. The system of claim 17, wherein said remote server updates a user profile in response to said user profile update information.

19. The system of claim 11, wherein said first user authentication occurs within an Intranet.

20. The system of claim 11, wherein said second user authentication occurs within said remote server.

21. A system for performing multiple user authentications with a single sign-on, comprising:

means for performing a first user authentication;

means for selecting a remote server subsequent to said first authentication;

means for sending a token to said remote server containing authentication information responsive to said first authentication; and

means for decoding said authentication information, wherein said means for decoding said authentication information induces a second user authentication.

22. A machine-readable medium having stored thereon instructions for performing multiple user authentications with a single sign-on, which, when executed by a set of processors, cause said set of processors to perform the following:

performing a first user authentication;

selecting a remote server subsequent to said first authentication;

sending a token to said remote server containing authentication information responsive to said first authentication; and

decoding said authentication information, wherein said decoding said authentication information induces a second user authentication.

ABSTRACT OF THE DISCLOSURE

A system and method for performing multiple user authentications with a single sign-on is disclosed. This system and method begins when the user performs a first user authentication, with user name and password, within the user's Intranet. Then the user selects a remote server subsequent to the first authentication. The server in the Intranet sends a token to the remote server containing authentication information made available because of the first authentication. Finally, the remote server decodes the authentication information, which has the effect within the remote server of performing a second user authentication without the user needing to sign-on a second time.

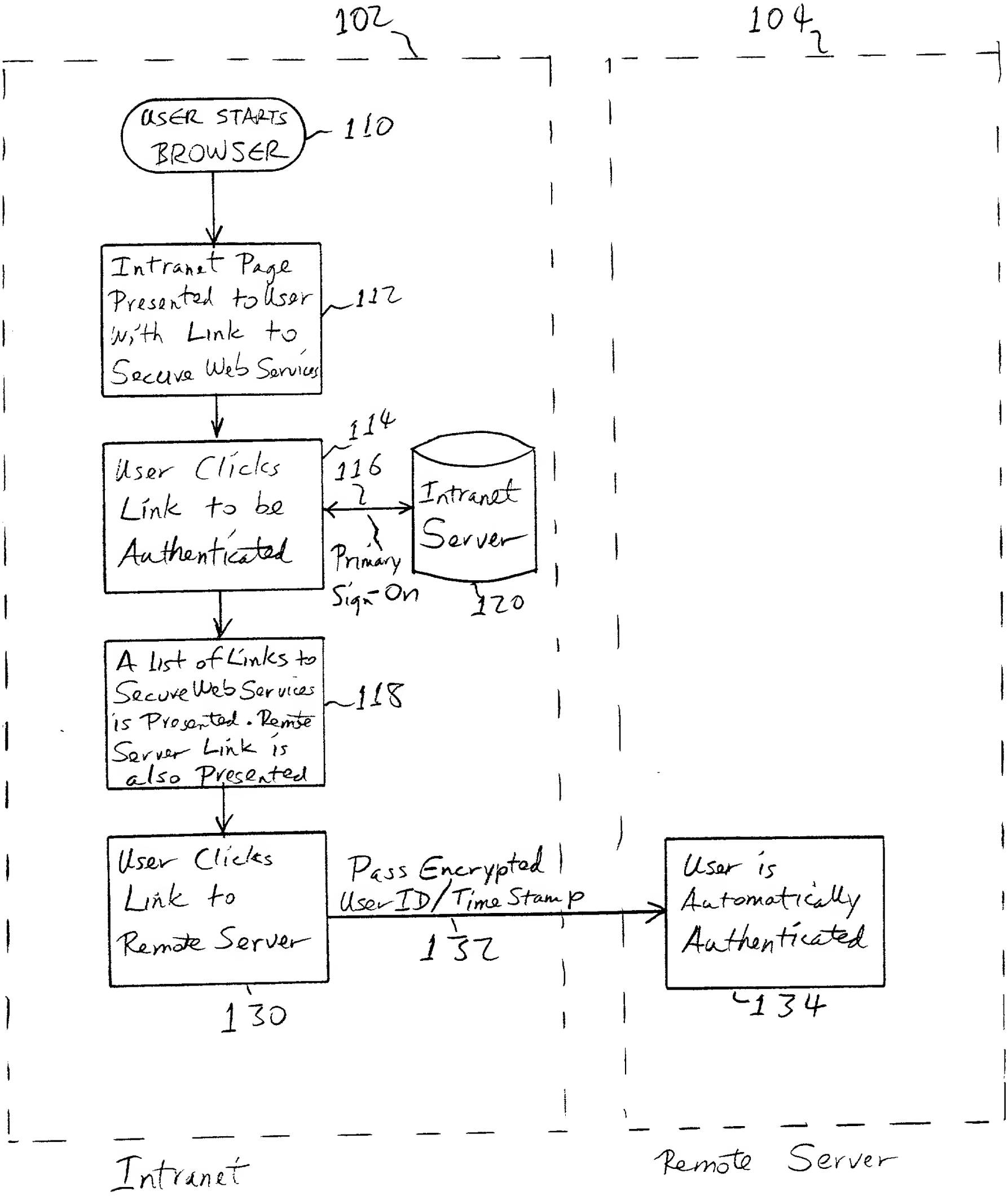
102
104
USER STARTS BROWSER
110
Intranet Page Presented to User With Link to Secure Web Services
112
User Clicks Link to be Authenticated
114
116
Primary Sign-On
Intranet Server
120
A list of Links to Secure Web Services is Presented. Remote Server Link is also Presented
118
User Clicks Link to Remote Server
130
Pass Encrypted User ID/Time Stamp
132
User is Automatically Authenticated
134
Intranet
Remote Server

FIGURE 1

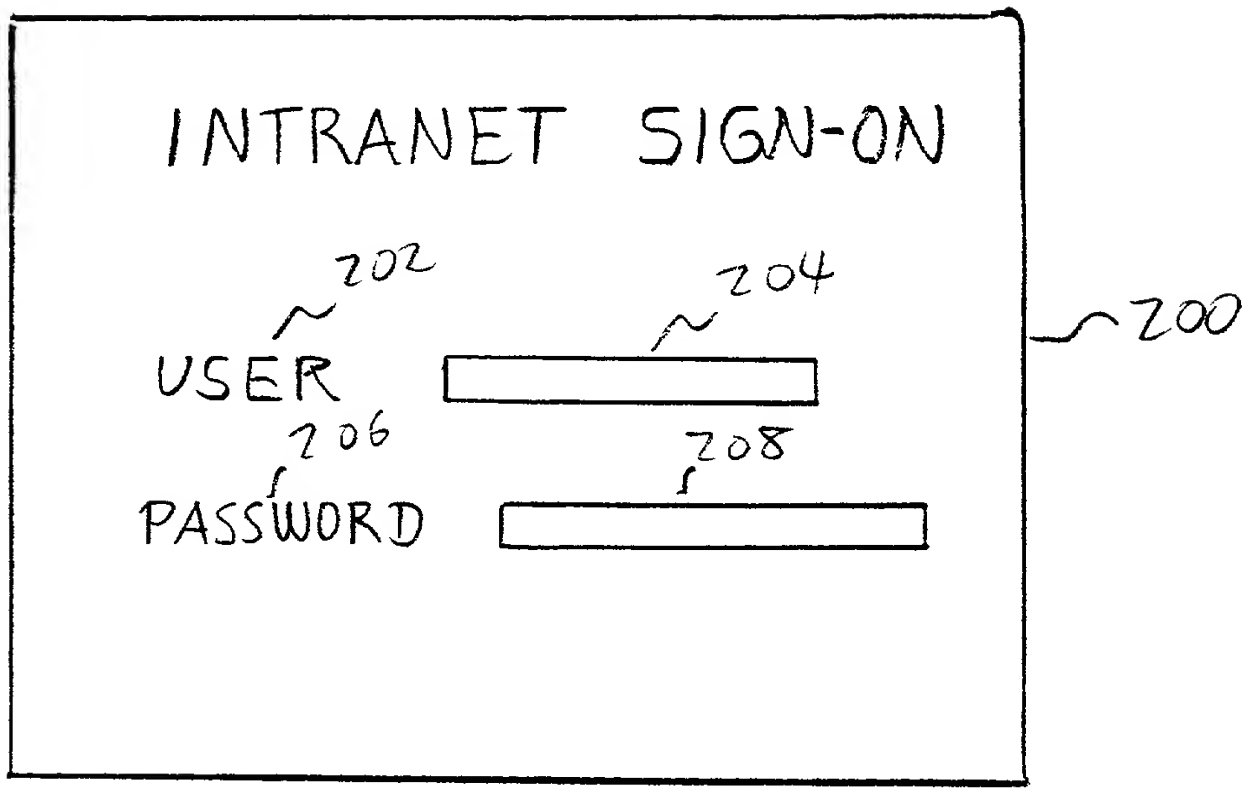

FIGURE 2A

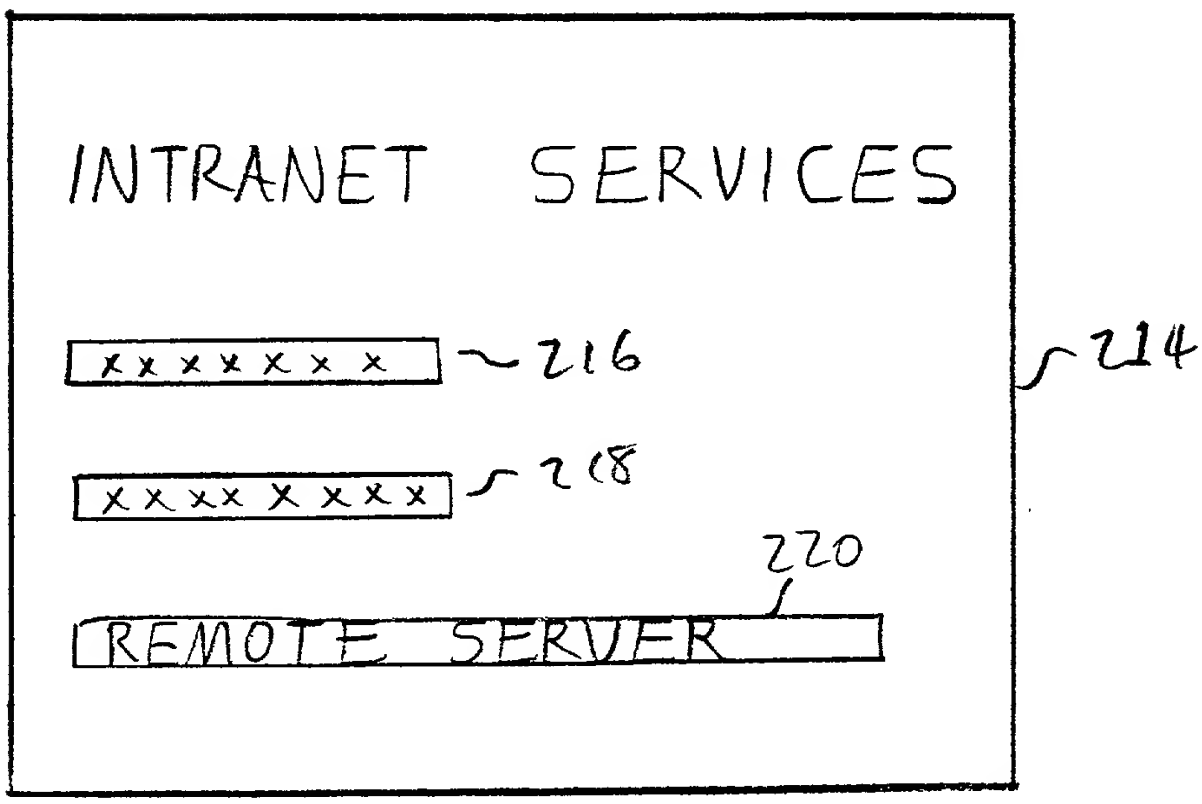

FIGURE 2B

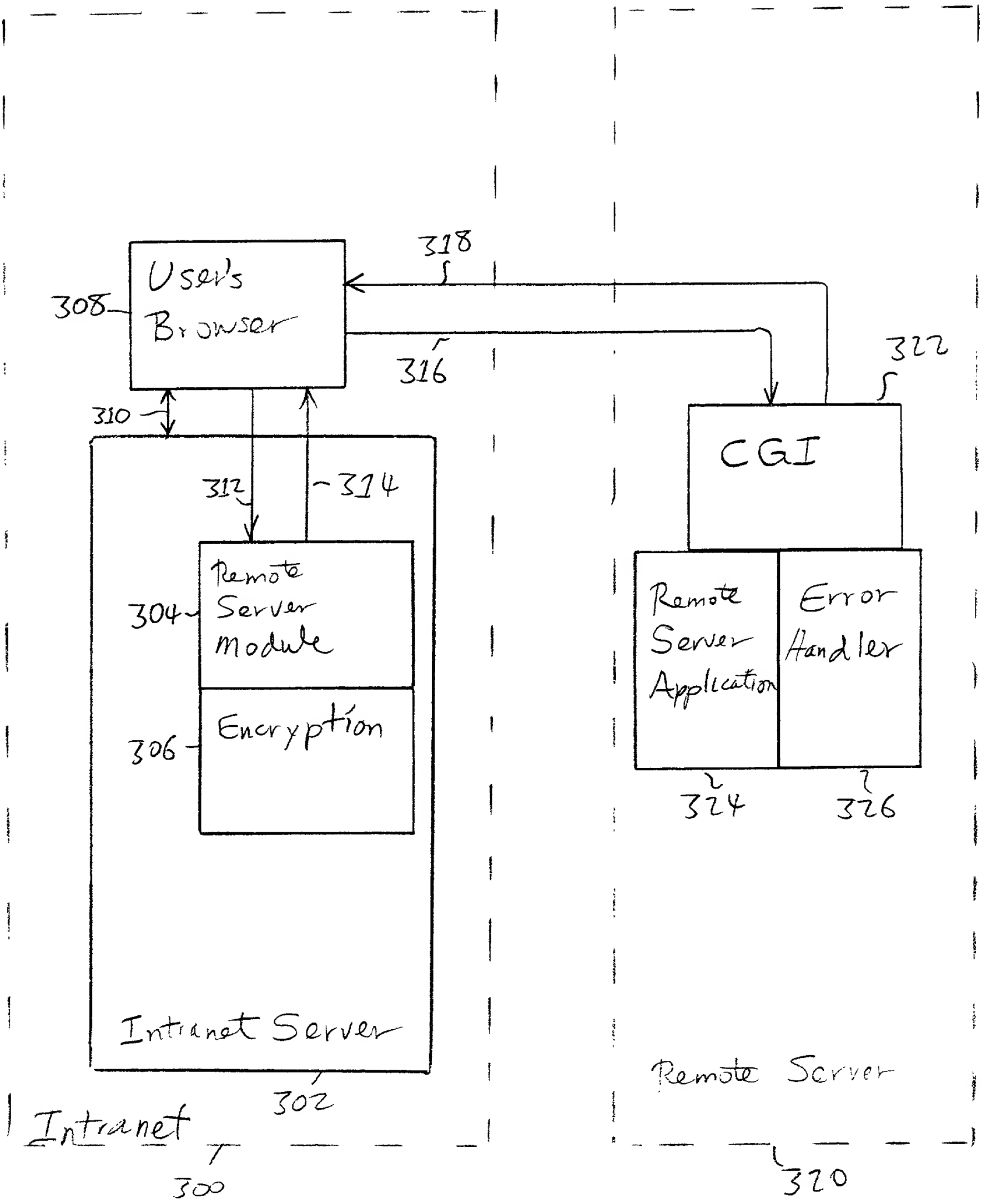
User's Browser
308
318
316
322
310
312
314
CGI
Remote Server Module
304
Encryption
306
Remote Server Application
Error Handler
324
326
Intranet Server
302
Remote Server
Intranet
300
320

FIGURE 3

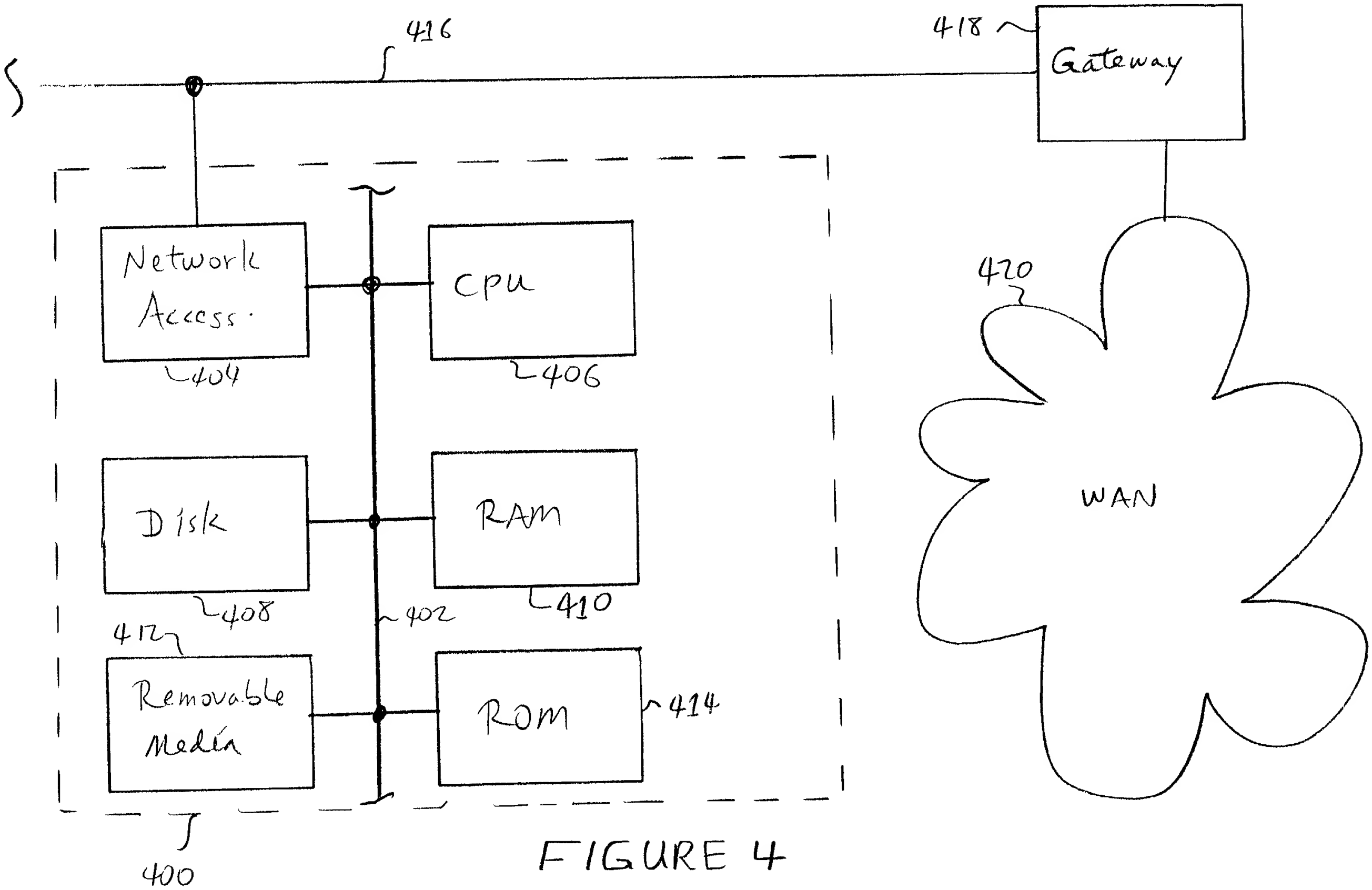

FIGURE 4

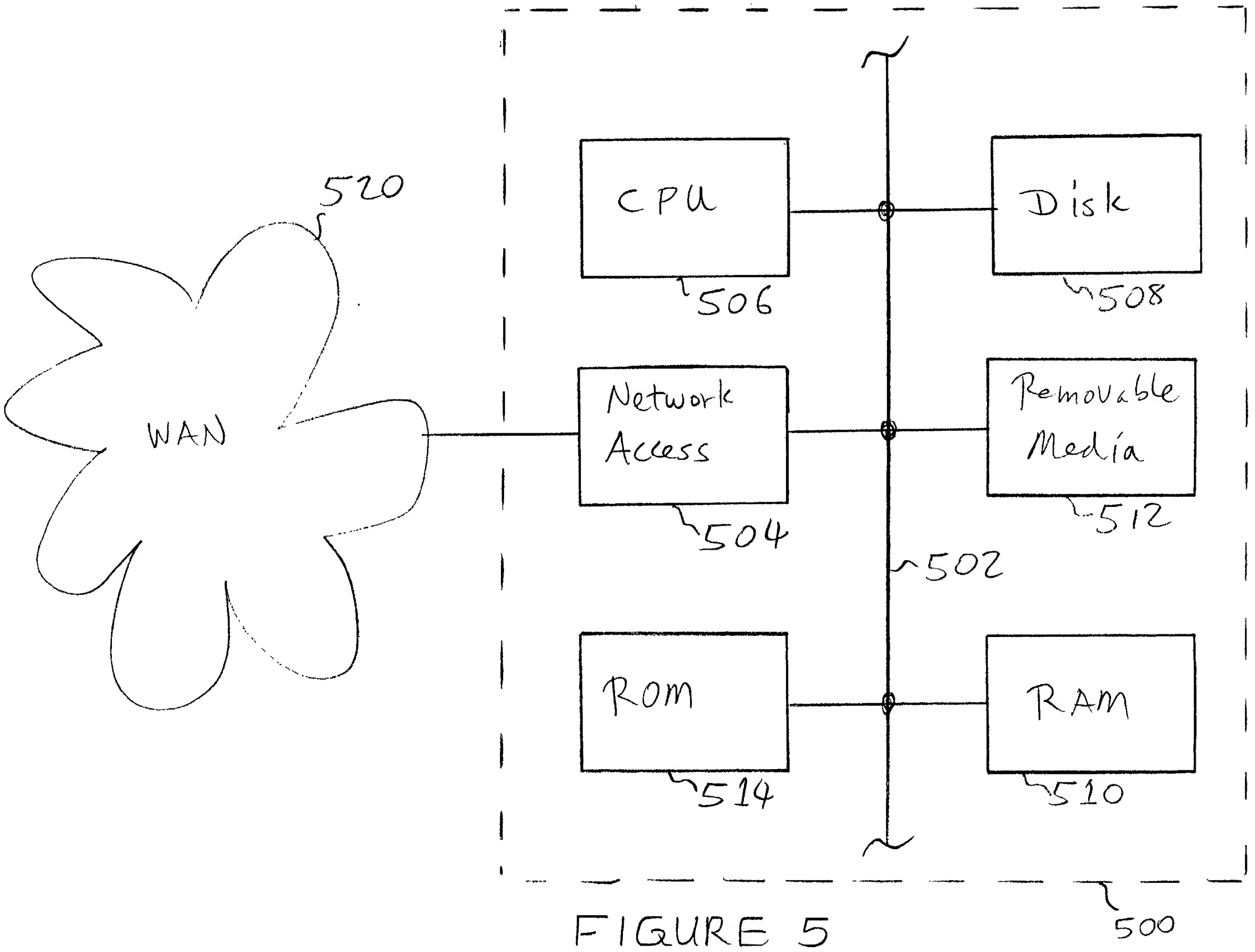

FIGURE 5

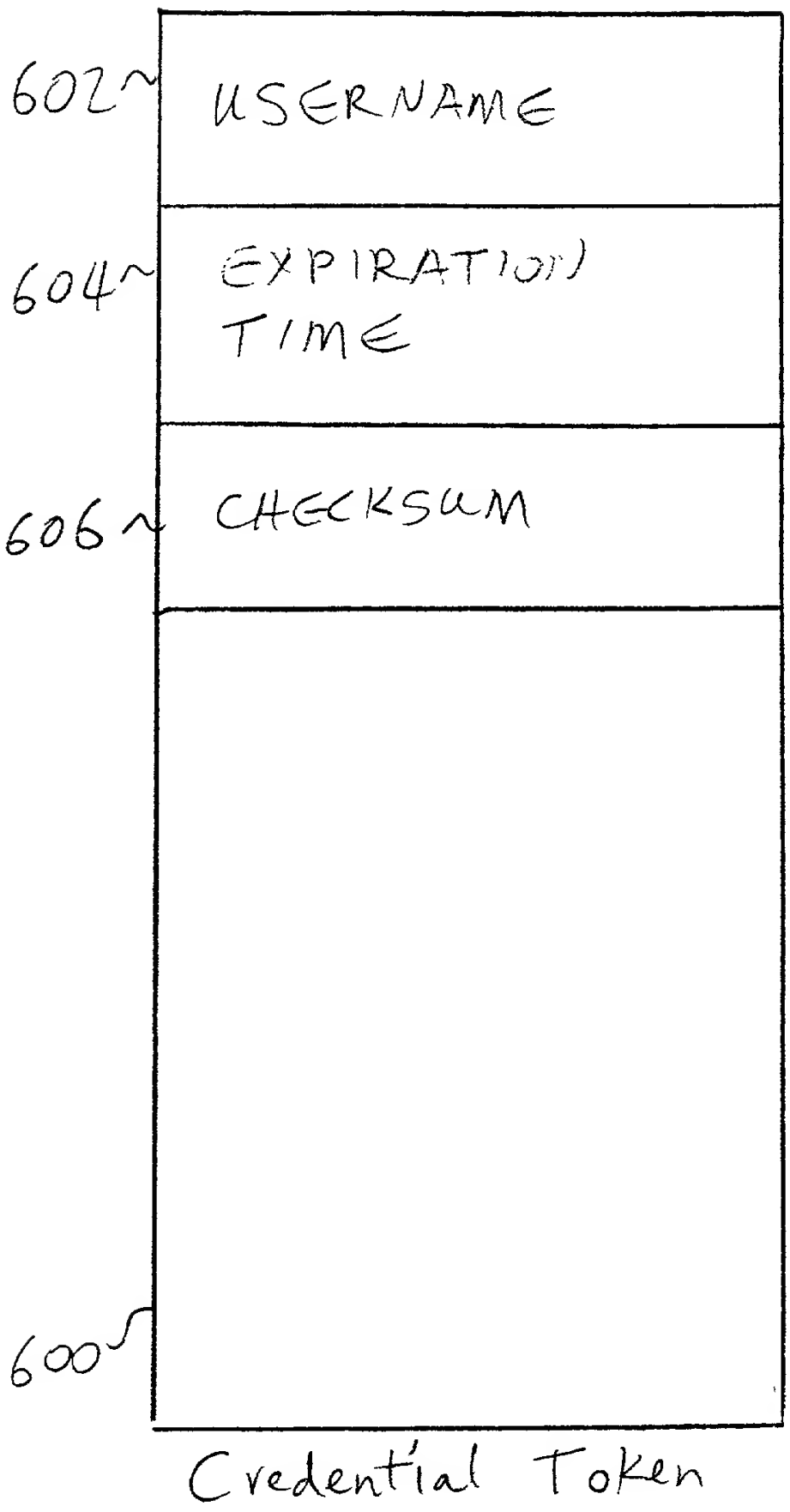
602
USERNAME
604
EXPIRATION TIME
606
CHECKSUM
600
Credential Token

FIGURE 6

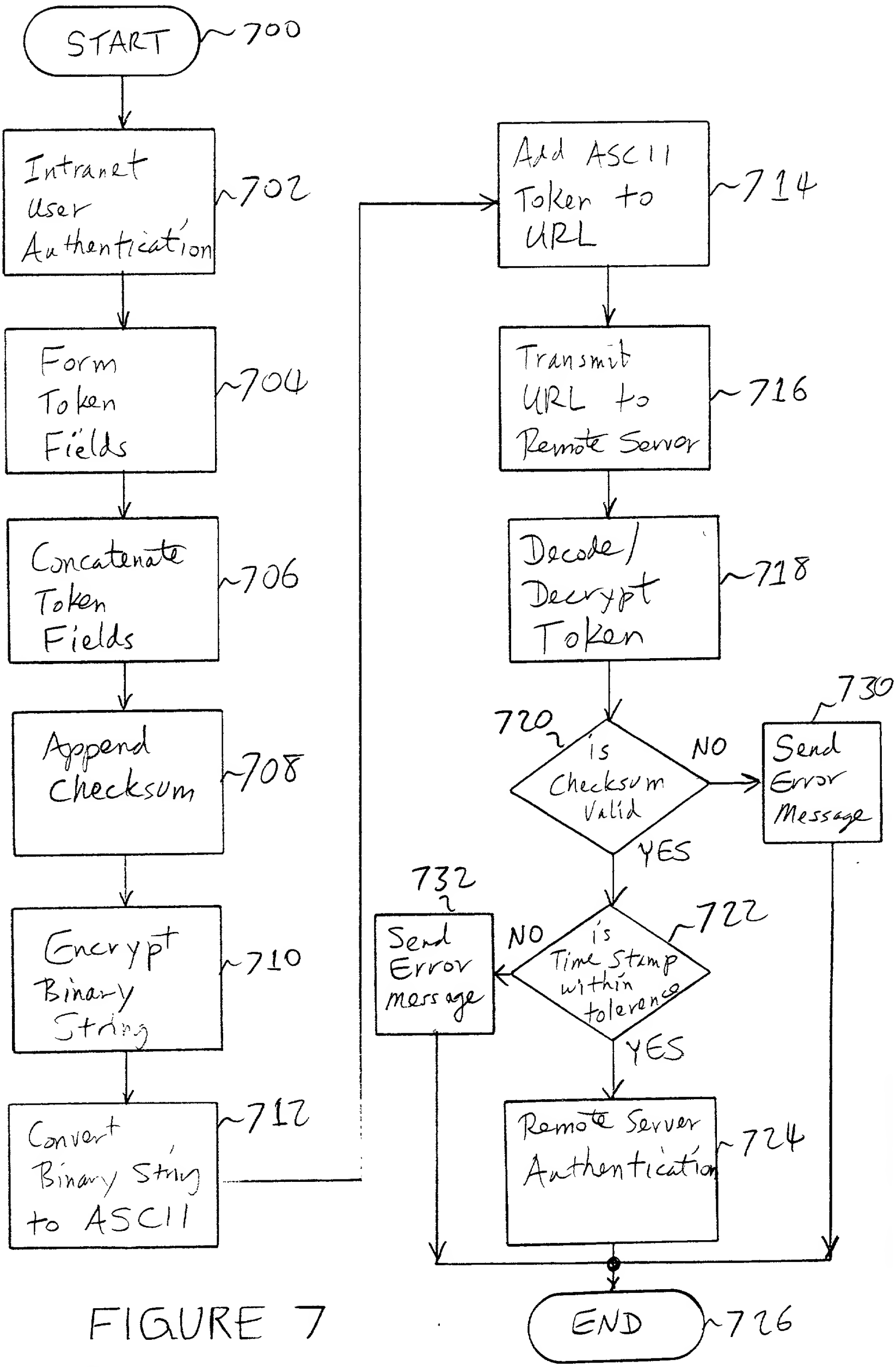
START
700
Intranet User Authentication
702
Form Token Fields
704
Concatenate Token Fields
706
Append Checksum
708
Encrypt Binary String
710
Convert Binary String to ASCII
712
Add ASCII Token to URL
714
Transmit URL to Remote Server
716
Decode/ Decrypt Token
718
730
720
Is Checksum Valid
NO
Send Error Message
YES
732
722
Send Error message
NO
Is Time Stamp within tolerance
YES
Remote Server Authentication
724
END
726

FIGURE 7

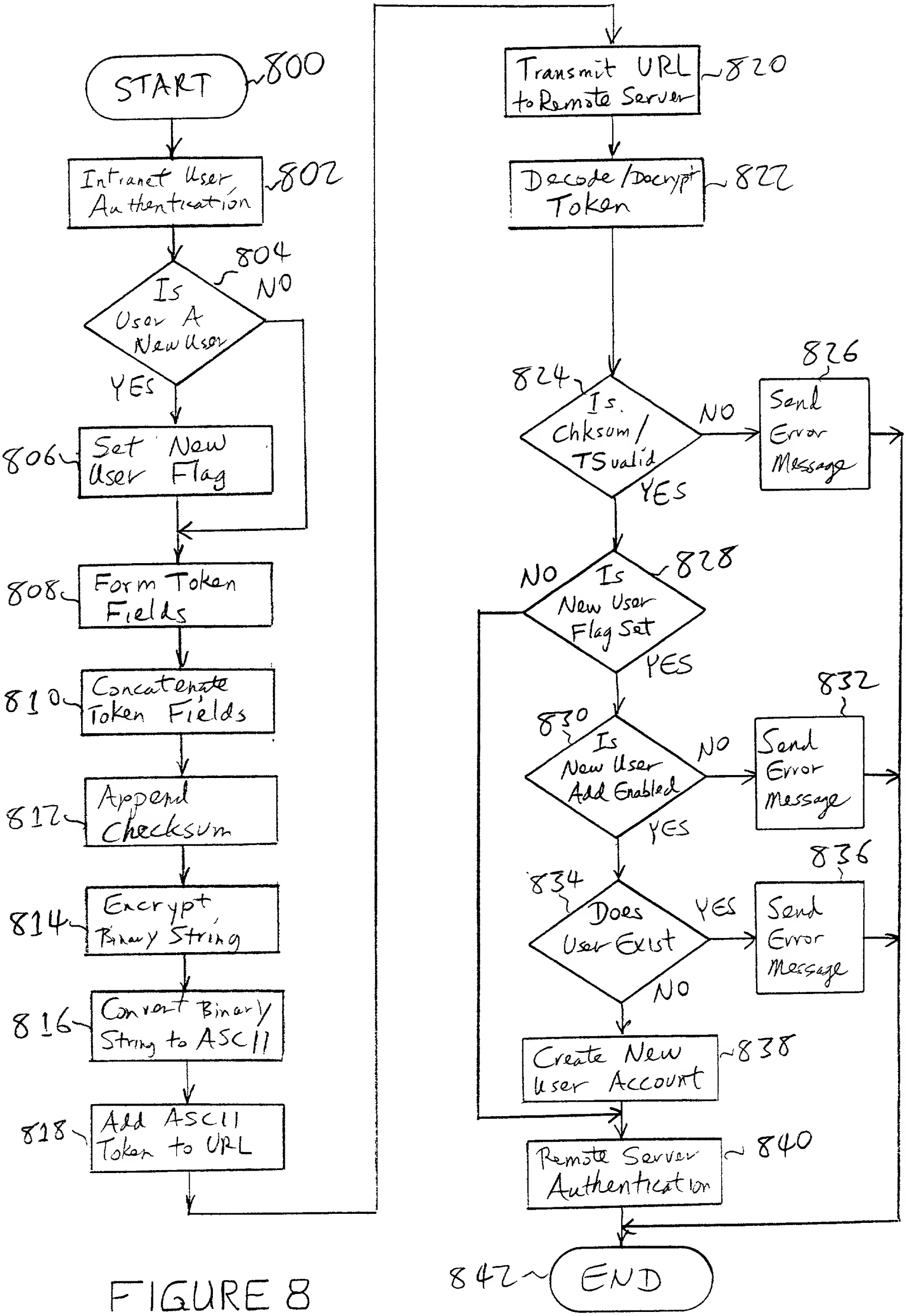
START
800
Intranet User Authentication
802
Is User A New User
804
NO
YES
Set New User Flag
806
Form Token Fields
808
Concatenate Token Fields
810
Append Checksum
812
Encrypt Binary String
814
Convert Binary String to ASCII
816
Add ASCII Token to URL
818
Transmit URL to Remote Server
820
Decode/Decrypt Token
822
Is Chksum/TS valid
824
NO
YES
Send Error Message
826
Is New User Flag Set
828
NO
YES
Is New User Add Enabled
830
NO
YES
Send Error Message
832
Does User Exist
834
YES
NO
Send Error Message
836
Create New User Account
838
Remote Server Authentication
840
END
842

FIGURE 8

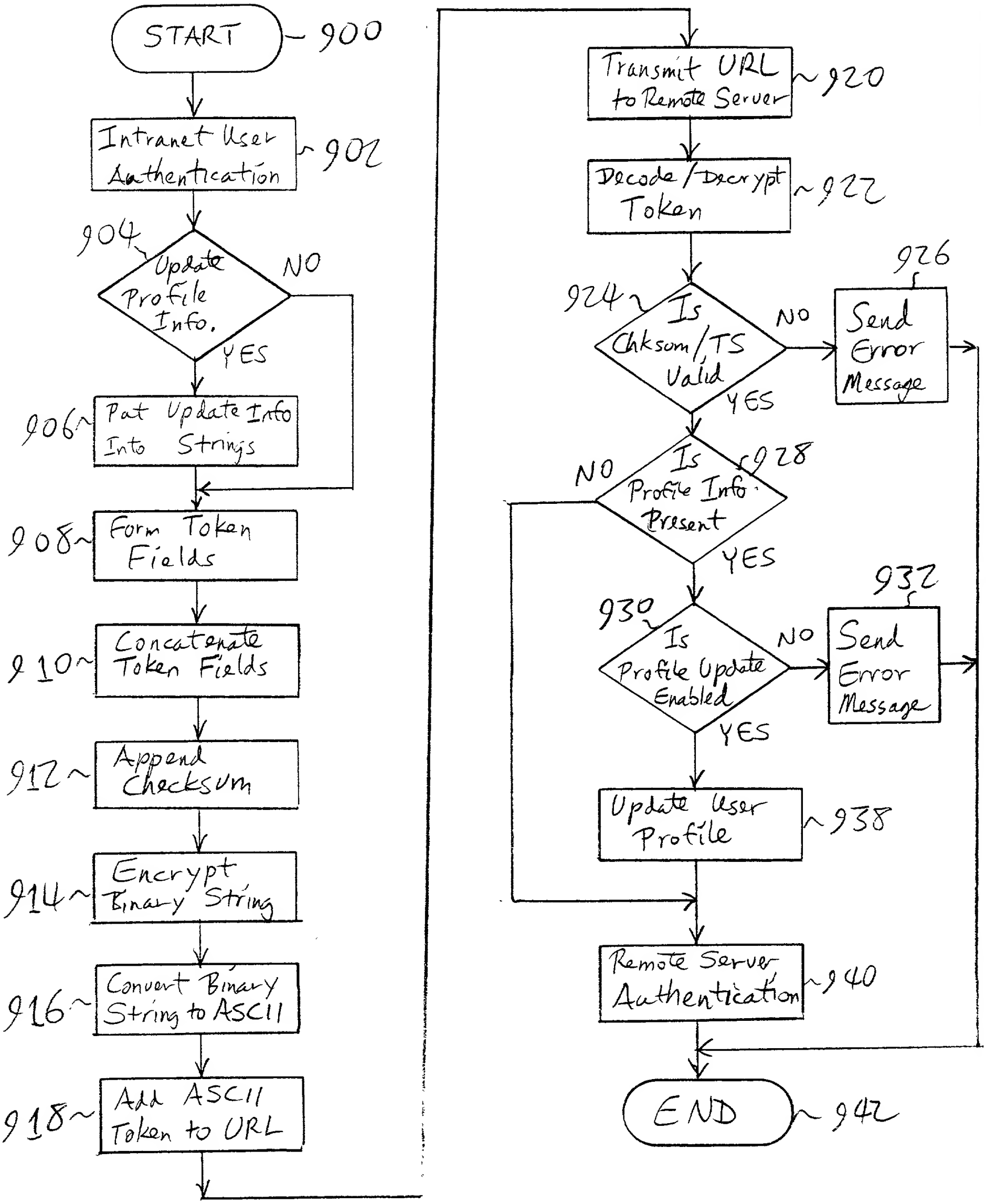
START
900
Intranet User Authentication
902
904
Update Profile Info.
NO
YES
906
Put Update Info Into Strings
908
Form Token Fields
910
Concatenate Token Fields
912
Append Checksum
914
Encrypt Binary String
916
Convert Binary String to ASCII
918
Add ASCII Token to URL
Transmit URL to Remote Server
920
Decode/Decrypt Token
922
924
Is Chksum/TS Valid
NO
YES
926
Send Error Message
928
Is Profile Info. Present
NO
YES
930
Is Profile Update Enabled
NO
YES
932
Send Error Message
938
Update User Profile
940
Remote Server Authentication
END
942

FIGURE 9

Attorney's Docket No.: 004701.P001 Patent

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

SYSTEM AND METHOD FOR ACCESSING A REMOTE SERVER FROM AN INTRANET WITH A SINGLE SIGN-ON

the specification of which

_X_ is attached hereto.
___ was filed on _____ as
United States Application Number _____
or PCT International Application Number _____
and was amended on _____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s) Priority Claimed

(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

(Application Number)	Filing Date
(Application Number)	Filing Date

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Number)	Filing Date	(Status -- patented, pending, abandoned)
(Application Number)	Filing Date	(Status -- patented, pending, abandoned)

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to Dennis A. Nicholls (Name of Attorney or Agent), BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, 12400 Wilshire Boulevard 7th Floor, Los Angeles, California 90025 and direct telephone calls to Dennis A. Nicholls (Name of Attorney or Agent), (408) 720-8300.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor Chee-Seng Chow

Inventor's Signature _____ Date _____

Residence San Jose, California (City, State) Citizenship Malaysia (Country)

Post Office Address 6268 Empress Court
San Jose, California 95129

Full Name of Second/Joint Inventor James Sung

Inventor's Signature _____ Date _____

Residence Fremont, California (City, State) Citizenship USA (Country)

Post Office Address 2261 Grapevine Terrace
Fremont, California 94539

Full Name of Third/Joint Inventor Jerome Tsung-Yao Chen

Inventor's Signature _____ Date _____

Residence Fremont, California (City, State) Citizenship USA (Country)

Post Office Address 47981 Avalon Heights Terrace
Fremont, California 94539

Full Name of Fourth/Joint Inventor Fiyaz Sundarji

Inventor's Signature _____ Date _____

Residence Los Altos, California (City, State) Citizenship USA (Country)

Post Office Address 881 Campbell Avenue
Los Altos, California 94024

APPENDIX A

William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. P42,261; Aloysius T. C. AuYeung, Reg. No. 35,432; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; Gregory D. Caldwell, Reg. No. 39,926; Ronald C. Card, Reg. No. 44,587; Andrew C. Chen, Reg. No. 43,544; Thomas M. Coester, Reg. No. 39,637; Alin Corie, Reg. No. P46,244; Dennis M. deGuzman, Reg. No. 41,702; Stephen M. De Klerk, under 37 C.F.R. § 10.9(b); Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Sanjeet Dutta, Reg. No. P46,145; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; Paramita Ghosh, Reg. No. 42,806; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Willmore F. Holbrow III, Reg. No. P41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; William W. Kidd, Reg. No. 31,772; Sang Hui Kim, Reg. No. 40,450; Eric T. King, Reg. No. 44,188; Erica W. Kuo, Reg. No. 42,775; Kurt P. Leyendecker, Reg. No. 42,799; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Darren J. Milliken, Reg. 42,004; Lisa A. Norris, Reg. No. 44,976; Chun M. Ng, Reg. No. 36,878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Daniel E. Ovanezian, Reg. No. 41,236; Marina Portnova, Reg. No. P45,750; Babak Redjaian, Reg. No. 42,096; William F. Ryann, Reg. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey Sam Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; John F. Travis, Reg. No. 43,203; George G. C. Tseng, Reg. No. 41,355; Joseph A. Twarowski, Reg. No. 42,191; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Mark L. Watson, Reg. No. P46,322; Thomas C. Webster, Reg. No. P46,154; Charles T. J. Weigell, Reg. No. 43,398; Kirk D. Williams, Reg. No. 42,229; James M. Wu, Reg. No. 45,241; Steven D. Yates, Reg. No. 42,242; and Norman Zafman, Reg. No. 26,250; my patent attorneys, and Justin M. Dillon, Reg. No. 42,486; my patent agent, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and James R. Thein, Reg. No. 31,710, my patent attorney.

APPENDIX B

Title 37, Code of Federal Regulations, Section 1.56
Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclosure information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclosure all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) Prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made or record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application;

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.